

CLAIMS

What is claimed is:

- 1 1. A method of providing encrypted data to a device comprising the steps of:
2 receiving one or more public keys from the device;
3 validating the one or more public keys;
4 receiving a request for the encrypted data from the device;
5 retrieving the encrypted data and a symmetric key used to encrypt the data;
6 encrypting the symmetric key using each of the one or more public keys; and
7 sending the one or more encrypted symmetric keys and the encrypted data to the
8 device.
- 1 2. The method as recited in claim 1, further comprising the steps of:
2 receiving data;
3 creating the symmetric key; and
4 encrypting the data using the symmetric key.
- 1 3. The method as recited in claim 2, further comprising the step of storing the symmetric
2 key and the encrypted data.
- 1 4. The method as recited in claim 2, wherein the data is compressed.
- 1 5. The method as recited in claim 4, wherein the data is compressed using a Moving
2 Picture Experts Groups ("MPEG") standard.

1 6. The method as recited in claim 2, further comprising the step of compressing the data.

1 7. The method as recited in claim 2, wherein the data is encrypted using a triple Data
2 Encryption Standard ("3DES") algorithm.

1 8. The method as recited in claim 2, wherein the data is encrypted using an Advanced
2 Encryption Standard ("AES") algorithm.

1 9. The method as recited in claim 1, wherein the data is encrypted using a symmetric
2 linear feedback shift register ("LFSR") sequence.

1 10. The method as recited in claim 1, further comprising the step of authorizing the
2 request.

1 11. The method as recited in claim 1, wherein the encrypted data includes one or more
2 terms of use.

1 12. The method as recited in claim 1, wherein the one or more terms of use comprises a
2 view only once restriction.

1 13. The method as recited in claim 1, wherein the one or more terms of use comprises a
2 limited time period to view the data.

1 14. The method as recited in claim 1, wherein the one or more terms of use comprises a
2 reproduction restriction.

1 15. The method as recited in claim 1, wherein the steps of encrypting the symmetric key
2 using each of the one or more public keys and sending the one or more encrypted symmetric
3 keys and the encrypted data to the device comprise the steps of:

4 encrypting the symmetric key and one or more terms of use using each of one or more
5 the public keys; and

6 sending the one or more encrypted symmetric keys, the one or more encrypted terms
7 of use and the encrypted data to the device.

1 16. The method as recited in claim 1, wherein the step of sending the one or more
2 encrypted symmetric keys and the encrypted data to the device comprises the steps of:

3 creating a file comprising the one or more encrypted symmetric keys and the
4 encrypted data; and

5 sending the file to the device.

1 17. The method as recited in claim 1, further comprising the step of establishing a
2 communication link with the device.

1 18. The method as recited in claim 1, wherein the communication link includes a
2 telephone line.

1 19. The method as recited in claim 1, wherein the communication link includes a wireless
2 connection.

1 20. The method as recited in claim 1, wherein the communication link includes a satellite
2 connection.

1 21. The method as recited in claim 1, wherein the communication link includes the
2 Internet.

1 22. The method as recited in claim 17, wherein the step of establishing a communication
2 link with the device comprises the steps of:

3 establishing a control communication link with the device; and
4 establishing a data communication link with the device.

1 23. The method as recited in claim 1, wherein the data is an audio/video transmission.

1 24. The method as recited in claim 1, wherein the data is a sound recording.

1 25. The method as recited in claim 1, wherein the data is a game.

1 26. The method as recited in claim 1, wherein the device is an audio/video playback
2 device.

1 27. The method as recited in claim 1, wherein the device is a computer.

- 1 28. The method as recited in claim 1, wherein the device is a personal data assistant.
- 1 29. The method as recited in claim 1, wherein the device is a wireless network device.

- 1 30. A computer program embodied on a computer readable medium of providing
2 encrypted data to a device comprising:
- 3 a code segment for receiving one or more public keys from the device;
 - 4 a code segment for validating the one or more public keys;
 - 5 a code segment for receiving a request for the encrypted data from the device;
 - 6 a code segment for retrieving the encrypted data and a symmetric key used to encrypt
7 the data;
 - 8 a code segment for encrypting the symmetric key using each of the one or more
9 public keys; and
 - 10 a code segment for sending the one or more encrypted symmetric keys and the
11 encrypted data to the device.
- 1 31. The computer program as recited in claim 30, further comprising:
- 2 a code segment for receiving data;
 - 3 a code segment for creating the symmetric key; and
 - 4 a code segment for encrypting the data using the symmetric key.
- 1 32. The computer program as recited in claim 31, further comprising a code segment for
2 storing the symmetric key and the encrypted data.
- 1 33. The computer program as recited in claim 31, wherein the data is compressed.

1 34. The computer program as recited in claim 33, wherein the data is compressed using a
2 Moving Picture Experts Groups ("MPEG") standard.

1 35. The computer program as recited in claim 31, further comprising a code segment for
2 compressing the data.

1 36. The computer program as recited in claim 31, wherein the data is encrypted using a
2 triple Data Encryption Standard ("3DES") algorithm.

1 37. The computer program as recited in claim 31, wherein the data is encrypted using an
2 Advanced Encryption Standard ("AES") algorithm.

1 38. The computer program as recited in claim 30, wherein the data is encrypted using a
2 symmetric linear feedback shift register ("LFSR") sequence.

1 39. The computer program as recited in claim 30, further comprising a code segment for
2 authorizing the request.

1 40. The computer program as recited in claim 30, wherein the encrypted data includes
2 one or more terms of use.

Patent 124143-1000

1 41. The computer program as recited in claim 30, wherein the one or more terms of use
2 comprises a view only once restriction.

1 42. The computer program as recited in claim 30, wherein the one or more terms of use
2 comprises a limited time period to view the data.

1 43. The computer program as recited in claim 30, wherein the one or more terms of use
2 comprises a reproduction restriction.

1 44. The computer program as recited in claim 30, wherein the code segments for
2 encrypting the symmetric key using each of the one or more public keys and sending the one
3 or more encrypted symmetric keys and the encrypted data to the device comprise:

4 a code segment for encrypting the symmetric key and one or more terms of use using
5 each of one or more the public keys; and

6 a code segment for sending the one or more encrypted symmetric keys, the one or
7 more encrypted terms of use and the encrypted data to the device.

1 45. The computer program as recited in claim 30, wherein the code segment for sending
2 the one or more encrypted symmetric keys and the encrypted data to the device comprises:

3 a code segment for creating a file comprising the one or more encrypted symmetric
4 keys and the encrypted data; and

5 a code segment for sending the file to the device.

1 46. The computer program as recited in claim 30, further comprising a code segment for
2 establishing a communication link with the device.

1 47. The computer program as recited in claim 30, wherein the communication link
2 includes a telephone line.

1 48. The computer program as recited in claim 30, wherein the communication link
2 includes a wireless connection.

1 49. The computer program as recited in claim 30, wherein the communication link
2 includes a satellite connection.

1 50. The computer program as recited in claim 30, wherein the communication link
2 includes the Internet.

1 51. The computer program as recited in claim 46, wherein the code segment for
2 establishing a communication link with the device comprises:

3 a code segment for establishing a control communication link with the device; and
4 a code segment for establishing a data communication link with the device.

1 52. The computer program as recited in claim 30, wherein the data is an audio/video
2 transmission.

1 53. The computer program as recited in claim 30, wherein the data is a sound recording.

1 54. The computer program as recited in claim 30, wherein the data is a game.

1 55. The computer program as recited in claim 30, wherein the device is an audio/video
2 playback device.

1 56. The computer program as recited in claim 30, wherein the device is a computer.

1 57. The computer program as recited in claim 30, wherein the device is a personal data
2 assistant.

3 58. The computer program as recited in claim 30, wherein the device is a wireless
4 network device.

1 59. A system for providing encrypted data to a device comprising:
2 a processor;
3 a data storage device communicably coupled to the processor;
4 a communications interface communicably coupled to the processor;
5 the processor receives one or more public keys from the device via the
6 communications interface, validates the one or more public keys, receives a request for the
7 encrypted data from the device via the communications interface, retrieves the encrypted data
8 and a symmetric key used to encrypt the data from the data storage device, encrypts the
9 symmetric key using each of the one or more public keys, and sends the one or more
10 encrypted symmetric keys and the encrypted data to the device via the communications
11 interface.

1 60. The system as recited in claim 59, wherein the processor receives data, creates the
2 symmetric key and encrypts the data using the symmetric key.

1 61. The system as recited in claim 60, wherein the processor stores the symmetric key
2 and the encrypted data in the data storage device.

1 62. The system as recited in claim 60, wherein the data is compressed.

1 63. The system as recited in claim 62, wherein the data is compressed using a Moving
2 Picture Experts Groups ("MPEG") standard.

- 1 64. The system as recited in claim 60, wherein the processor compresses the data.
- 1 65. The system as recited in claim 60, wherein the data is encrypted using a triple Data
2 Encryption Standard (“3DES”) algorithm.
- 1 66. The system as recited in claim 60, wherein the data is encrypted using an Advanced
2 Encryption Standard (“AES”) algorithm.
- 1 67. The system as recited in claim 59, wherein the data is encrypted using a symmetric
2 linear feedback shift register (“LFSR”) sequence.
- 1 68. The system as recited in claim 59, wherein the processor authorizes the request.
- 1 69. The system as recited in claim 59, wherein the encrypted data includes one or more
2 terms of use.
- 1 70. The system as recited in claim 59, wherein the one or more terms of use comprises a
2 view only once restriction.
- 1 71. The system as recited in claim 59, wherein the one or more terms of use comprises a
2 limited time period to view the data.

1 72. The system as recited in claim 59, wherein the one or more terms of use comprises a
2 reproduction restriction.

1 73. The system as recited in claim 59, wherein the processor encrypts one or more terms
2 of use using each of one or more the public keys and sends the one or more encrypted terms
3 of use to the device via the communications interface.

1 74. The system as recited in claim 59, wherein the processor sends the one or more
2 encrypted symmetric keys and the encrypted data to the device by creating a file comprising
3 the one or more encrypted symmetric keys and the encrypted data, and sending the file to the
4 device via the communications interface.

1 75. The system as recited in claim 59, the processor establishes a communication link
2 between the communications interface and the device.

1 76. The system as recited in claim 59, wherein the communication link includes a
2 telephone line.

1 77. The system as recited in claim 59, wherein the communication link includes a
2 wireless connection.

1 78. The system as recited in claim 59, wherein the communication link includes a satellite
2 connection.

1 79. The system as recited in claim 59, wherein the communication link includes the
2 Internet.

1 80. The system as recited in claim 75, wherein processor establishes a communication
2 link between the communications interface and the device by establishing a control
3 communication link between the communications interface and the device and establishing a
4 data communication link between the communications interface and the device.

1 81. The system as recited in claim 59, wherein the data is an audio/video transmission.

1 82. The system as recited in claim 59, wherein the data is a sound recording.

1 83. The system as recited in claim 59, wherein the data is a game.

1 84. The system as recited in claim 59, wherein the device is an audio/video playback
2 device.

1 85. The system as recited in claim 59, wherein the device is a computer.

1 86. The system as recited in claim 59, wherein the device is a personal data assistant.

1 87. The system as recited in claim 59, wherein the device is a wireless network device.